honest Consulting

dnslogger

Echtzeit DNS Protokollierung

dnslogger

- registriert DNS Verkehr
- speichert DNS Nachrichten lokal oder leitet sie via TCP an ein Ziel weiter
- sendet im Format Syslog oder JSON
- schlichtes, kostenloses Werkzeug von VendorN Ltd

dnslogger

- Einsatz auf autoritativen oder rekursiven DNS Servern
- ist herstellerunabhängig
- sparsam im Betrieb
- Unterstützt IPv4, TCP und UDP
  - IPv6, DoT, DoH, … in Entwicklung
- braucht keine zusätzlichen Treiber
- Automatischer Failover

hc

Testumgebung

	Linux	**Windows**	**Ziel**
OS	Cent OS 7	Win Server 2016	macOS
DNS	BIND	Win DNS	-/-
Format	Syslog	JSON	Beide
IP	172.16.79.138	172.16.79.140	172.16.79.1

dnslogger Linux

https://youtu.be/AEWzpqltIhQ

dnslogger Mac

https://youtu.be/u9ZQGkobwHM

dnslogger Windows

https://youtu.be/OMUwk50-Rj0

dnslogger

- Integration in DNS-Infrastruktur als Datenquelle für SIEM-Lösung
- Generelles Logging von DNS Aktivitäten

Thank you for your Time.

https://honest-consulting.de/for-you/

hc